Revision Letter

Editor: Jaehoon (Paul) Jeong
Date: August 30, 2021

Hi Pascal,
I sincerely appreciate your keen and productive comments to improve our draft. I have addressed your comments below. My answers start with a prefix "=> [PAUL]".

Reviewer: Pascal Thubert
Review result: Not Ready

Dear authors

In summary:

I read a number of very good drafts collated in one, from the use cases that very complete and ready to publish, to the architecture and protocol solution in section 4 that would require more work for completeness.

There are multiple instances in the use cases where protocols are listed coming out of the blue, e.g., the references to OMNI that seem artificially spread regardless of the context of the section. OMNI is used throughout, both as an open ended toolbox, and as a carpet under which all problems can be hidden.

Reading this doc, OMNI shows as an interface to a software mobile router, with multiple of the device physical interfaces connected to the mobile router. This makes the stack very simple as the complexity moves to the router. But now you have to implement the router. Presented as that, the OMNI router deserves its name, it's indeed very rich; it seems to cover all forms of MANET (many to choose from) and NEMO (and all the MIP protocol family across address families), all the possible radio interfaces on which the ND problems go away by magic, and whatever else you want to put in there. Is that the intention?
=> [PAUL] No, that is not the intention. I have reflected the comments of the author, Fred Templin, of the OMNI draft during the IPWAVE WG Last Call.

Instead of referring to OMNI for virtually anything, the doc should refer to MANET for MANET things (like BYOD), NEMO for NEMO things (like MNP), draft-nordmark-intarea-ippl for split subnets, and draft-thubert-6man-ipv6-over-wireless for P2MP/NBMA link and subnet models. And then you can say that all those components

can be plugged in the OMNI router, and you can discuss which MANET and which MIP you want, including using OMNI's built in mobility.
=> [PAUL] I agree with you on this matter.

Note that my objections are not against the OMNI design, it might be the perfect thing and I am already aware of use cases that could be served by a P2MP interface like OMNI in conjunction with RFC8505 on the P2P subinterfaces (recycling the high level design we've been shipping for IPv4 / frame relay for the last 30 years). My objection is of the way the draft uses [OMNI] as the magic wand that solves all the problems when what you really do is throw them over the fence. I'd rather you focus on problems and use cases, for which there's excellent text, and indicate what needs to be done without making assumption on how the needful things will be solved.
=> [PAUL] I remove the text related to the OMNI from the revision by focusing on the problems and use cases along with the requirements and without any assumption on the specific protocol operations.

In agreement with a discussion on the 6MAN list, I'd suggest to split, keep all that's use case and problem description and ship it, remove references to protocols envisioned in the solution, and start the work on architecture of the solution and the protocol applicability statements separately. An alternate would be to centralize the discussion on protocols to annex, and explain that protocol A or B could be envisioned in solution space because to over this gap or implement that function.
=> [PAUL] I remove references to protocols envisioned in the solution from the main text.

In any fashion, the current text is not ready for publication as applicability statement, architecture and or/solution, so the related work should be removed from the main text. But I find it mostly ready for use case and problem statement, more below.
=> [PAUL] I edit this draft to have only use cases and problem statement rather than applicability statement, architecture and solution.

Review:

Abstract

> **This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation Systems (ITS).**

>>> The document goes beyond that; there was actually a thread at 6MAN where Bob Hinden said " This document says it is a problem statement, but then becomes a solution document. Might be better to cut it down to only the problem statement part. " >>> Would you consider doing this? If not, why? Note: you may want to respond on 6MAN as well. >>> >>>I would have thought that the

traditional steps of problem statement and applicability statement of existing work could be expected from IPWAVE too. >>> Please clarify the steps that you intend to follow next with this work.
=> [PAUL] I have revised this draft such that it becomes a problem statement rather than a solution document.

<snip>

1. Introduction

>>> Very readable and informative section, many thanks!

Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Locator/ID Separation Protocol (LISP) [RFC6830BIS], and Asymmetric Extended Route Optimization (AERO) [RFC6706BIS]).

>>> NEMO (RFC 3963) is not cited. Any reason why the vehicle would not transport a network?
=> [PAUL] I add NEMO (RFC 3963) to the above sentence as follows.

NEW
Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Network Mobility (NEMO) [RFC3963], Locator/ID Separation Protocol (LISP) [RFC6830BIS], and Asymmetric Extended Route Optimization (AERO) [RFC6706BIS]). In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6][ISO-ITS-IPv6-AMD1].

<snip>

This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then enumerates requirements for the extensions of those IPv6 protocols, which are

tailored to IPv6-based vehicular networking. Thus, this document is intended to motivate development of key protocols for IPWAVE.

>>>

<snip>

2. Terminology

>>>

<snip>

o IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motor cycle, and a similar one) and a device (e.g., smartphone and IoT device). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. See the definition of the term "OBU" in [RFC8691].

>>> Can that be a router connecting multiple computers?
=> [PAUL] That can be a router connecting multiple computers inside a vehicle. The updated text is as follows.

NEW
o IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motor cycle, and a similar one) and a device (e.g., smartphone and IoT device). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. It can play a role of a router connecting multiple computers (or in-vehicle devices) inside a vehicle. See the definition of the term "OBU" in [RFC8691].

<snip>

3. Use Cases

>>> This is another great read and an enlightening section. Maybe mention in the abstract that the doc also covers use cases?
=> [PAUL] The abstract mentions that this document covers use cases.

CURRENT
This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document explains use cases using V2V, V2I, and V2X networking. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then enumerates requirements for the extensions of those IPv6 protocols for IPv6-based vehicular networking.

<snip>

Although a Layer-2 solution can provide a support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as 5G V2X and DSRC. Therefore, the existing IPv6 protocol can be augmented through the addition of an Overlay Multilink Network (OMNI) Interface [OMNI] and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard in a highway having multiple kinds of radio technologies, such as 5G V2X and DSRC.

>>> This text appears in the middle of high level use case, with a crude list of protocols; this is not a place for it
=> [PAUL] This text is removed from the V2V use case to explain the operations of V2V under multiple L2 technologies. It is moved to Appendix A as follows.

Appendix A. Support of Multiple Radio Technologies for V2V

NEW
Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide a support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., Overlay Multilink Network (OMNI) Interface [OMNI]) and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications

to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.

>>> On a 6MAN Thread, Brian Carpenter said that the above:
“
is of concern regardless of the mention of OMNI. Does it mean "can be" or "needs to be"? This paragraph seems like a very short summary of a big problem area. At the end of page 13 there is some related discussion, which mentions RPL as part of the solution (good choice, IMHO) but again seems to depend on OMNI. I don't think the fix of simply removing references to OMNI works, because it would leave a gap. In an informational document, that is not a formal problem but as far as this draft describes architecture, I don't think that big a gap is reasonable. "OMNI" is mentioned more than 20 times in the document. There are also several references to AERO, which is strongly associated with OMNI. “ >>> I agree with Brian. Here the document seems to be mixing solution with problem and putting the cart before the horse. My recommendation is to stick to what needs to be done that IPv6 does not do yet -the reqs and gaps-; but the doc should not step in the how things will be done unless the group already decided to do it. The logical next steps to a PS are an applicability statement of existing work, and if the gaps cannot be filled, there may be one or more WG chartered to fill those gaps.
=> [PAUL] I modified this draft not to have a solution from the main text, and a solution is replaced in an annex.
Section 3.1. V2V

OLD
Although a Layer-2 solution can provide a support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as 5G V2X and DSRC. Therefore, the existing IPv6 protocol can be augmented through the addition of an Overlay Multilink Network (OMNI) Interface [OMNI] and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard in a highway having multiple kinds of radio technologies, such as 5G V2X and DSRC. To support applications of these V2V use cases, the functions of IPv6 such as VND and VSP are prerequisites for IPv6-based packet exchange and secure, safe communication between two vehicles.

Section 3.1. V2V

NEW

To support applications of these V2V use cases, the required functions of IPv6 include IPv6-based packet exchange and secure, safe communication between two vehicles. For the support of V2V under multiple radio technologies (e.g., DSRC and 5G V2X), refer to Appendix A.

Appendix A. Support of Multiple Radio Technologies for V2V

NEW
Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide a support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., Overlay Multilink Network (OMNI) Interface [OMNI]) and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.

>>> I'd still be happy to see an annex with leads on where the solution might come from like RFC 8691 does.

=> A solution for V2V use case under multiple radio technologies is replaced in an annex as follows.

Appendix A. Support of Multiple Radio Technologies for V2V

NEW
Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide a support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., Overlay Multilink Network (OMNI) Interface [OMNI]) and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.

<snip>

The existing IPv6 protocol must be augmented through the addition of an OMNI interface and/or protocol changes in order to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles. Thus, IPv6 needs to be extended for multihop V2I communications.

>>> Note that I have no clue on how well OMNI applies in that space, maybe it does very well; but here it comes out of the blue with no justification. If you mention OMNI you need to detail what it is and which of the V2V problems you expect it to solve. But then, that's beyond the scope of a PS.
=> [PAUL] I delete the OMNI from the text so that the protocol changes can include a virtual interface such as OMNI.

Section 3.2. V2I

OLD
The existing IPv6 protocol must be augmented through the addition of an OMNI interface and/or protocol changes in order to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles. Thus, IPv6 needs to be extended for multihop V2I communications.

Section 3.2. V2I

NEW
The existing IPv6 protocol must be augmented through protocol changes in order to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles. Thus, IPv6 needs to be extended for multihop V2I communications.

<snip>

The existing IPv6 protocol must be augmented through the addition of an OMNI interface and/or protocol changes in order to support wireless multihop V2X (or V2I2X) communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles (or pedestrians' smartphones). Thus, IPv6 needs to be extended for multihop V2X (or V2I2X) communications.

>>> Please be more specific on what the missing functions are and whether they are missing from the stack development standpoint or if there's work needed from the IETF.
1) If something is really missing in our specs, the text to prove from the use case

above is missing 2) how OMNI serves the use case could be elaborated in an applicability statement of OMNI for V2xyz, but it is a bit blunt to present it as panacea when the problems to be solved are not listed. 3) If you look at it, OMNI seems like a software mobile router within a bump in the stack. Can that become too big?
=> [PAUL] I delete the OMNI from the text to let this draft focus on the problems rather than a solution.

Section 3.3. V2X

OLD
The existing IPv6 protocol must be augmented through the addition of an OMNI interface and/or protocol changes in order to support wireless multihop V2X (or V2I2X) communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles (or pedestrians' smartphones). Thus, IPv6 needs to be extended for multihop V2X (or V2I2X) communications.

Section 3.3. V2X

NEW
The existing IPv6 protocol must be augmented through protocol changes in order to support wireless multihop V2X or V2I2X communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles (or pedestrians' smartphones) as packet forwarders. Thus, IPv6 needs to be extended for multihop V2X or V2I2X communications.

>>> my view is that the text above and the similar occasions should be replaced by something like :

The existing IPv6 protocol must be augmented to provide the following functions: 1) …
=> [PAUL] I have addressed this in the previous comment.

>>> and / or something like:

In addition to the IPv6 node requirements [RFC 8504], the IPv6 protocol stack for use in a vehicle must support 1) RFC blah, 2) …
=> [PAUL] I have addressed this in the previous comment.

<snip>

To support applications of these V2X use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisites for IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

>>> "the functions of IPv6 such as VND, VMM, and VSP" does not parse. There's no IPv6 reference that provides those functions. If the intention is to say that there's stuff to add to IPv6 to support, like, say, VND, then this document fails to define how an IPv6 VND should behave, though it's precisely what I'd expect from a problem statement.
=> I delete the usage of VND, VMM, and VSP from the text as follows.

Section 3.3. V2X

OLD
To support applications of these V2X use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisites for IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

Section 3.3. V2X

NEW
To support applications of these V2X use cases, the required functions of IPv6 include IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

<snip>

4. Vehicular Networks

>>> What is the purpose of section 4 as a whole, problem statement or applicability statement of the listed protocols? In the former case what's the problem? In the latter case it is incomplete and needs to be exported to an applicability statement doc with all the possible technologies evaluated.
==> (Chris)
Section 4 defines an overall architecture for vehicular networks. Based on the architecture for V2V, V2I, and V2X, we then state several issues in Section 5. If we do not have the architecture, the issues discussed in Section 5 will be difficult to understand.

This section describes an example vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks.

>>> I read this as presenting a context to explain what the problems are instead of presenting the IPVAWE "architecture". Maybe using the term "Architecture" here is misleading and led to Bob's comment.
==> (Chris)
We replaced the "architecture" term with "context" for clarity.

Section 4

OLD
This section describes an example vehicular network architecture supporting V2V, V2I, and V2X communications ~~in vehicular networks~~. It describes an internal network within a vehicle or an edge network (called EN). It explains not only the internetworking between the internal networks of a vehicle and an EN via wireless links, but also the internetworking between the internal networks of two vehicles via wireless links.

Section 4

NEW
This section describes the context for vehicular networks supporting V2V, V2I, and V2X communications. It describes an internal network within a vehicle or an edge network (called EN). It explains not only the internetworking between the internal networks of a vehicle and an EN via wireless links, but also the internetworking between the internal networks of two vehicles via wireless links.

<snip>

4.1. Vehicular Network Architecture

Figure 1 shows an example vehicular network architecture for V2I and V2V in a road network [OMNI].

a. Is using OMNI a decision that the WG made for the future work ? what does it do and what does it not do?
b. Is there work left to be done? Who will do that work? Or is it the expectation that OMNI has it all defined already?
==> [PAUL] OMNI architecture is proposed in 6man WG but not a WG draft, and currently it is in the ISE (Independent Submission Editor) process for an independent submission. To reduce the confusion, we minimize the contents related to OMNI architecture here and delete Figure 2.

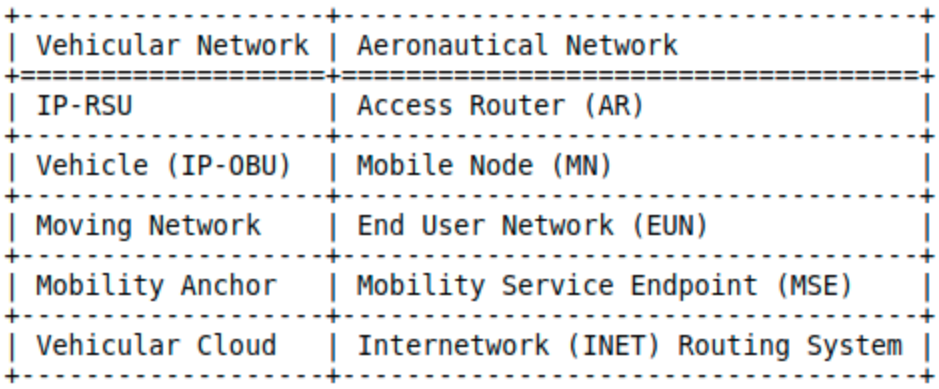
Section 4.1, 1st paragraph

OLD
Figure 1 shows an example vehicular network architecture for V2I and V2V in a road network ~~[OMNI]~~. The vehicular network architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components. ~~Note that the components of the vehicular network architecture can be mapped to those of an IP-based aeronautical network architecture in [OMNI], as shown in Figure 2.~~

Section 4.1, 1st paragraph

NEW
Figure 1 shows an example vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components.

Figure 2 is deleted:



Vehicular Network	Aeronautical Network
IP-RSU	Access Router (AR)
Vehicle (IP-OBU)	Mobile Node (MN)
Moving Network	End User Network (EUN)
Mobility Anchor	Mobility Service Endpoint (MSE)
Vehicular Cloud	Internetwork (INET) Routing System

Figure 2: Mapping between Vehicular Network Components and Aeronautical Network Components

<snip>

An existing network architecture (e.g., an IP-based aeronautical network architecture [OMNI][UAM-ITS], a network architecture of PMIPv6 [RFC5213], and a low-power and lossy network architecture [RFC6550]) can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. In a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). For example, the OMNI interface and/or RPL (IPv6 Routing

Protocol for Low-Power and Lossy Networks) [RFC6550] can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

>>> all this could fit well in annex; anyway you need to explain what you expect the protocols to do and which extension is needed. In the case of RPL at least you indicate that it would do routing, but not why you cannot use it of the shelf; for OMNI, what you expect is less clear, though there's text elsewhere about the many radio interfaces that could be used for the purpose, and the text in the UAM below that is enlightening.

==> [PAUL] We removed the contents related to OMNI. We made Appendix B to explain the support of multihop V2X networking with RPL and OMNI.

Section 4.1. Vehicular Network Architecture

OLD
An existing network architecture (e.g., ~~an IP-based aeronautical network architecture [OMNI][UAM-ITS],~~ a network architecture of PMIPv6 [RFC5213], and a low-power and lossy network architecture [RFC6550]) can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. In a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). For example, the ~~OMNI interface and/or~~ RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

Section 4.1. Vehicular Network Architecture

NEW
Existing network architectures, such as the network architectures of PMIPv6 [RFC5213], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550], and OMNI (Overlay Multilink Network Interface) [OMNI], can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. Refer to Appendix B for the detailed discussion on multihop V2X networking by RPL and OMNI.

Appendix B. Support of Multihop V2X Networking

NEW
The multihop V2X networking can be supported by RPL (IPv6 Routing Protocol for

Low-Power and Lossy Networks) [RFC6550] and Overlay Multilink Network (OMNI) Interface [OMNI].

RPL defines an IPv6 routing protocol for low-power and lossy networks (LLN), mostly designed for home automation routing, building automation routing, industrial routing, and urban LLN routing. It uses a destination oriented directed acyclic graph (DODAG) to construct routing paths for hosts in a network. The DODAG uses an objective function (OF) for route selection and optimization within the network. A user can use different routing metrics to define an OF for a specific scenario. RPL supports multipoint-to-point, point-to-multipoint, and point-to-point traffic, and the major traffic flow is the multipoint-to-point traffic. For example, in a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). In this case, the RPL can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

OMNI defines the transmission of IPv6 packets over Overlay Multilink Network Interfaces that are virtual interfaces governing multiple physical network interfaces. OMNI supports multihop V2V communication between vehicles in multiple forwarding hops via intermediate vehicles with OMNI links. It also supports multihop V2I communication between a vehicle and an infrastructure access point by multihop V2V communication. The OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD Messaging.

==> [PAUL] We explain why we cannot use RPL of the shelf in Section 5.1.3 as follows.

Section 5.1.3. Routing

NEW
RPL [RFC6550] defines a routing protocol for low-power and lossy networks, which constructs and maintains DODAGs optimized by an Objective Function (OF). A defined OF provides route selection and optimization within a RPL topology. A node in a DODAG uses DODAG Information Objects (DIOs) messages to discover and maintain the upward routes toward the root node. An address registration extension for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) in [RFC8505] can support light-weight mobility for nodes moving through different parents. Mainly it updates the Address Registration Option (ARO) of ND defined in [RFC6775] to include a status field that can indicate the movement of a node and optionally a Transaction ID (TID) field, i.e., a sequence number that can be used to determine the most recent location of a node. RPL can use the information provided by the extended ARO defined in [RFC8505] to deal with a certain level of node mobility. When a leaf node moves to the coverage of another parent node, it should de-register its addresses to the previous parent node and register itself

with a new parent node along with an incremented TID.

Although RPL can be used in IPv6-based vehicular networks, it is primarily designed for lossy networks, which puts energy efficiency first. In addition, the topology it considers may not quickly scale up and down for IPv6-based vehicular networks, since the mobility of vehicles is much more diverse with a high speed, so it can frequently alter a tree-like topology formed by RPL, which may cause network fragmentation and merging with more control traffic.

Moreover, due to bandwidth and energy constraints, RPL does not suggest to use a proactive mechanism (e.g., keepalive) to maintain accurate routing adjacencies such as Bidirectional Forwarding Detection [RFC5881] and MANET Neighborhood Discovery Protocol [RFC6130]. As a result, due to the mobility of vehicles, the network fragmentation is not detected quickly and the routing of packets between vehicles or between a vehicle and an infrastructure node may fail.

<snip>

To support not only the mobility management of the UAM end systems, but also the multihop and multilink communications of the UAM interfaces, the UAM end systems can employ an Overlay Multilink Network (OMNI) interface [OMNI] as a virtual Non-Broadcast Multiple Access (NBMA) connection to a serving ground domain infrastructure.

>>> Again, what is the expectation for OMNI? As an overlay it requires an underlay; when connecting to a MANET it needs support for that MANET. The text above seems to imply that is solves everything in V2xyz like magic; reminds me of the IPv6 multicast abstraction that was supposed to solve the broadcast problem and ended up worsening it.
==> [PAUL] We have removed the contents related to OMNI here because our draft focuses on the problems in IP-based vehicular networking.

<snip>

This infrastructure can be configured over the underlying data links. The OMNI interface and its link model provide a means of multilink, multihop and mobility coordination to the legacy IPv6 ND messaging [RFC4861] according to the NBMA principle. Thus, the OMNI link model can support efficient UAM internetworking services without additional mobility messaging, and without any modification to the IPv6 ND messaging services or link model.

>>> Again, what is the expectation for OMNI? As an overlay it requires an underlay; the text above seems to imply that is solves everything in V2xyz like magic; that would be a

stretch, that reminds me of IPv6 multicast that was supposed to solve the broadcast problem and ended up worsening it.
==> [PAUL] Along with the previous comment, we have removed the contents related to OMNI here.

Section 4.1, the 3rd paragraph (deleted)

OLD
~~Wireless communications needs to be considered for end systems for Urban Air Mobility (UAM) such as flying cars and taxis [UAM-ITS]. These UAM end systems may have multiple wireless transmission media interfaces (e.g., cellular, communications satellite (SATCOM), short-range omni-directional interfaces), which are offered by different data link service providers. To support not only the mobility management of the UAM end systems, but also the multihop and multilink communications of the UAM interfaces, the UAM end systems can employ an Overlay Multilink Network (OMNI) interface [OMNI] as a virtual Non-Broadcast Multiple Access (NBMA) connection to a serving ground domain infrastructure. This infrastructure can be configured over the underlying data links. The OMNI interface and its link model provide a means of multilink, multihop and mobility coordination to the legacy IPv6 ND messaging [RFC4861] according to the NBMA principle. Thus, the OMNI link model can support efficient UAM internetworking services without additional mobility messaging, and without any modification to the IPv6 ND messaging services or link model.~~

<snip>

Multiple vehicles under the coverage of an RSU share a prefix just as mobile nodes share a prefix of a Wi-Fi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2, and Vehicle5) can use Prefix 1 to configure their IPv6 global addresses for V2I communication. Alternatively, mobile nodes can employ an OMNI interface and use their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network without requiring the messaging of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862], which uses an on-link prefix provided by the (visited) wireless LAN; this technique is known as "Bring-Your-Own-Addresses".

>>> Is OMNI the only way to "Bring-Your-Own-Addresses"? Else the text could be more generic, at least use e.g., like the ref to AERO later.
==> [PAUL] We delete the reference to OMNI for a generic way for “Bring-Your-Own-Addresses (BYOA)”.

>>> What are the implications / limitations of doing that – like they can do line of sight V2V but not reach the internet, or the need of a local MANET / RPL that will accept to route those addresses, or the security / address ownership validation issues ?
==> [PAUL] We have revised the contents here to make a more generic statement by removing the text related to OMNI. The purpose of using the way, “Bring-Your-Own-Addresses (BYOA)”, is to reduce the control traffic (e.g., DAD) imposed by the normal SLAAC and its related operations.

Section 4.1, 4th paragraph

OLD
Multiple vehicles under the coverage of an RSU share a prefix just as mobile nodes share a prefix of a Wi-Fi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2, and Vehicle5) can use Prefix 1 to configure their IPv6 global addresses for V2I communication. Alternatively, mobile nodes can employ an OMNI interface and use their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network without requiring the messaging of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862], which uses an on-link prefix provided by the (visited) wireless LAN~~; this technique is known as "Bring-Your-Own-Addresses"~~.

Section 4.1, 4th paragraph

NEW
Multiple vehicles under the coverage of an RSU share a prefix just as mobile nodes share a prefix of a Wi-Fi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2, and Vehicle5) can use Prefix 1 to configure their IPv6 global addresses for V2I communication. Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" technique using their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network, which does not require the messaging (e.g., Duplicate Address Detection (DAD)) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862].

<snip>

A single subnet prefix announced by an RSU can span multiple vehicles in VANET. For example, in Figure 1, for Prefix 1, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) can construct a connected VANET. Also, for Prefix 2, two vehicles (i.e., Vehicle3 and Vehicle6) can construct another connected VANET, and for Prefix 3, two vehicles (i.e., Vehicle4 and Vehicle7) can construct another connected VANET. Alternatively, each vehicle could employ an OMNI interface with their own ULAs such that no topologically-oriented subnet prefixes need be announced by the RSU.

>>> same as above. This seems to restate the same thing, derive an address from a topologically correct prefix or use your own with limitations to be described.
==> (Chris)
We agree with the reviewer's comment and we delete this paragraph to remove confusion.

Section 4.1, the 6th paragraph

OLD
~~A single subnet prefix announced by an RSU can span multiple vehicles in VANET. For example, in Figure 1, for Prefix 1, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) can construct a connected VANET. Also, for Prefix 2, two vehicles (i.e., Vehicle3 and Vehicle6) can construct another connected VANET, and for Prefix 3, two vehicles (i.e., Vehicle4 and Vehicle7) can construct another connected VANET. Alternatively, each vehicle could employ an OMNI interface with their own ULAs such that no topologically-oriented subnet prefixes need be announced by the RSU.~~

<snip>

For IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. An Ethernet Adaptation (EA) layer is in charge of transforming some parameters between the IEEE 802.11 MAC layer and the IPv6 network layer, which is located between the IEEE 802.11-OCB's logical link control layer and the IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IPv6-based vehicular networks.

>>> solution space.
==> (Chris)
Since IEEE 802.11-OCB is primarily designed for vehicular networks and RFC 8691 is the basic definition for it and not a solution, problems stated in this draft are based on this RFC. This is the reason that we put RFC 8691 here. Nevertheless, we reduce the contents here to remove confusion.
We also noticed that the description about RFC8691 is not accurate, so the text is updated as follows.

Section 4.1,

OLD
For IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. ~~An Ethernet Adaptation (EA) layer is in charge of transforming some parameters between the~~

~~IEEE 802.11 MAC layer and the IPv6 network layer, which is located between the IEEE 802.11-OCB's logical link control layer and the IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IPv6-based vehicular networks.~~

Section 4.1,

NEW
As a basic definition for IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure.

<snip>

An IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle's TCP session can be continued, or UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a corresponding node in the vehicular cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213] and AERO [RFC6706BIS]).

In the host-based mobility scheme (e.g., MIPv6), an IP-RSU plays a role of a home agent. On the other hand, in the network-based mobility scheme (e.g., PMIPv6, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, which also serves vehicles as a home agent, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs client functionality in IPv6 stack of a vehicle as a mobile node for mobility signaling message exchange between the vehicle and home agent. On the other hand, the network-based mobility scheme does not need such a client functionality for a vehicle because the network infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent handles the mobility signaling message exchange with the home agent (e.g., LMA in PMIPv6) for the sake of the vehicle.

There are a scalability issue and a route optimization issue in the network-based mobility scheme (e.g., PMIPv6) when an MA covers a large vehicular network governing many IP-RSUs. In this case, a distributed mobility scheme (e.g., DMM [RFC7429]) can mitigate the scalability issue by distributing multiple MAs in the vehicular network such that they are positioned closer to vehicles for route optimization and bottleneck mitigation in a

central MA in the network-based mobility scheme. All these mobility approaches (i.e., a host-based mobility scheme, network-based mobility scheme, and distributed mobility scheme) and a hybrid approach of a combination of them need to provide an efficient mobility service to vehicles moving fast and moving along with the relatively predictable trajectories along the roadways.

In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding by using the concept of Software-Defined Networking (SDN) [RFC7149][DMM-FPC]. Note that Forwarding Policy Configuration (FPC) in [DMM-FPC], which is a flexible mobility management system, can manage the separation of data-plane and control-plane in DMM. In SDN, the control plane and data plane are separated for the efficient management of forwarding elements (e.g., switches and routers) where an SDN controller configures the forwarding elements in a centralized way and they perform packet forwarding according to their forwarding tables that are configured by the SDN controller. An MA as an SDN controller needs to efficiently configure and monitor its IP-RSUs and vehicles for mobility management, location management, and security services.

The mobility information of a GPS receiver mounted in its vehicle (e.g., position, speed, and direction) can be used to accommodate mobility-aware proactive handover schemes, which can perform the handover of a vehicle according to its mobility and the wireless signal strength of a vehicle and an IP-RSU in a proactive way.

Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275] and PMIPv6 [RFC5213], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. IP tunneling over the wireless link should be avoided for performance efficiency. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

>>> This is all very informative text but does not state a problem. Is there a problem is left to be solved or are we assessing the applicability of protocols? Could it for instance, forward point to issues discussed in section 5?
==> [PAUL] The text of the existing approaches for mobility management is moved to Appendix C.

Section 4.1

OLD
An IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle's TCP session can be continued, or UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU's

wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a corresponding node in the vehicular cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213] and AERO [RFC6706BIS]).

Appendix C. Support of Mobility Management for V2I

NEW

The seamless application communication between two vehicles or between a vehicle and an infrastructure node requires mobility management in vehicular networks. The mobility management schemes include a host-based mobility scheme, network-based mobility scheme, and software-defined networking scheme.

In the host-based mobility scheme (e.g., MIPv6), an IP-RSU plays a role of a home agent. On the other hand, in the network-based mobility scheme (e.g., PMIPv6, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, which also serves vehicles as a home agent, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs client functionality in IPv6 stack of a vehicle as a mobile node for mobility signaling message exchange between the vehicle and home agent. On the other hand, the network-based mobility scheme does not need such a client functionality for a vehicle because the network infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent handles the mobility signaling message exchange with the home agent (e.g., LMA in PMIPv6) for the sake of the vehicle.

There are a scalability issue and a route optimization issue in the network-based mobility scheme (e.g., PMIPv6) when an MA covers a large vehicular network governing many IP-RSUs. In this case, a distributed mobility scheme (e.g., DMM [RFC7429]) can mitigate the scalability issue by distributing multiple MAs in the vehicular network such that they are positioned closer to vehicles for route optimization and bottleneck mitigation in a central MA in the network-based mobility scheme. All these mobility approaches (i.e., a host-based mobility scheme, network-based mobility scheme, and distributed mobility scheme) and a hybrid approach of a combination of them need to provide an efficient mobility service to vehicles moving fast and moving along with the relatively predictable trajectories along the roadways.

In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding by using the concept of Software-Defined Networking (SDN) [RFC7149][DMM-FPC]. Note that Forwarding Policy Configuration (FPC) in [DMM-FPC], which is a flexible mobility management system, can manage the separation of data-plane and control-plane in DMM. In SDN, the control plane and data plane are separated for the efficient management of forwarding elements (e.g., switches and routers) where an SDN controller configures the forwarding elements in a centralized way and they perform

packet forwarding according to their forwarding tables that are configured by the SDN controller. An MA as an SDN controller needs to efficiently configure and monitor its IP-RSUs and vehicles for mobility management, location management, and security services.

<snip>

As shown in Figure 3, as internal networks, a vehicle's moving network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. The internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks. For the efficiency, the network prefixes of the internal networks (as a moving network) in a vehicle need to be delegated and configured automatically. Note that a moving network's network prefix can be called a Mobile Network Prefix (MNP) [OMNI].

>>> Then again you're overselling OMNI. MNP is originally defined here https://datatracker.ietf.org/doc/html/rfc3963#section-2 and that's a reference you can use normatively.
==> [PAUL] We replace the OMNI reference with RFC3963 for NEMO.

Section

OLD
As shown in Figure 3, as internal networks, a vehicle's moving network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. The internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks. For the efficiency, the network prefixes of the internal networks (as a moving network) in a vehicle need to be delegated and configured automatically. Note that a moving network's network prefix can be called a Mobile Network Prefix (MNP) ~~[OMNI]~~.

Section

NEW
As shown in Figure 3, as internal networks, a vehicle's moving network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. The

internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks. For the efficiency, the network prefixes of the internal networks (as a moving network) in a vehicle need to be delegated and configured automatically. Note that a moving network's network prefix can be called a Mobile Network Prefix (MNP) [RFC 3963].

<snip>

As shown in Figure 3, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be either global IPv6 addresses, or IPv6 ULAs as long as IPv6 packets can be routed within vehicular networks [OMNI].

>>> Then again you're overselling OMNI. There needs to be a routing protocol like a MANET that will accept to carry the MNPs, and that must be implemented by the infra and both cars. The OMNI spec is clear on that. This is why at first glance I see OMNI as a full mobile router in a bump in the stack. Now what is the problem behind this? No such protocol at IETF? Too many to choose from? No deployment?

==> [PAUL] Thanks for pointing this out. We removed the OMNI reference. We focus on the IPv6 addressing problem (link-local IPv6 addresses, ULAs, or global IPv6 addresses) for V2I as follows.

Section 4.2

OLD
As shown in Figure 3, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be either global IPv6 addresses~~, or IPv6 ULAs as long as IPv6 packets can be routed within vehicular networks [OMNI]~~.

Section 4.2

NEW
As shown in Figure 3, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be link-local IPv6 addresses, ULAs, or global IPv6 addresses.

<snip>

When global IPv6 addresses are used, wireless interface configuration and control overhead for Duplicate Address Detection (DAD) [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways; when ULAs and the OMNI interface are used, no DAD nor MLD messaging is needed.

>>> Then again you're overselling OMNI. Isn't it the no dad needed a property of injecting a BYOA in the fabric for an GUA MIP Home Address which is known to be unique at home?
>>> OTOH, autoconf'ing a random ULA "FD…"prefix has lesser DAD properties than autoconf'ing a random 64bit IID in a classical subnet. So who says DAD isn't required for OMNI ULA?
>>> note that IMHO DAD on wireless is a lot more harm than good, and I agree that with a good pseudo random generator the ULA has no chance to collision in the real world, as OMNI claims. It's just that your argument here plays the other way, because there are less random bits (56) in the ULA prefix than in the IID (62), and if one starts using more prefix bits to be non-random, there will be a time when DAD on prefix is needed.
==> (Chris)
We agree with the reviewer on this point, and we removed the contents related to ULAs and OMNI.

Section 4.2

OLD
When global IPv6 addresses are used, wireless interface configuration and control overhead for Duplicate Address Detection (DAD) [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways~~; when ULAs and the OMNI interface are used, no DAD nor MLD messaging is needed~~.

Section 4.2

NEW
When global IPv6 addresses are used, wireless interface configuration and control overhead for DAD [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways.

<snip>

Let us consider the upload/download time of a vehicle when it passes through the wireless communication coverage of an IP-RSU. For a given typical setting where 1km is the maximum DSRC communication range [DSRC] and 100km/h is the speed limit in highway, the dwelling time can be calculated to be 72 seconds by dividing the diameter

of the 2km (i.e., two times of DSRC communication range where an IP-RSU is located in the center of the circle of wireless communication) by the speed limit of 100km/h (i.e., about 28m/s). For the 72 seconds, a vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU.

<snip>

4.3. V2V-based Internetworking

>>> In this section it looks like the cars are in a stable line of sight relationship. Which is probably fine for a platoon, but when you drive along with friends in different cars, you realize that the line of sight assumption does not stand over time. Soon enough, other cars meddle in, and possibly one of the cars drives faster and too far ahead so you need the infra to relay, possibly over multiple infra hops.
==> [PAUL] In this section, the link between two vehicles is assumed to be stable for single-hop wireless communication regardless of the sight relationship such as line of sight and non-line of sight, as shown in Figure 3. Even in Figure 4, the three vehicles are connected to each other with a linear topology, however, our multihop V2V communication can accommodate any network topology, that is, an arbitrary graph.

Section 4.3

NEW
In this section, the link between two vehicles is assumed to be stable for single-hop wireless communication regardless of the sight relationship such as line of sight and non-line of sight, as shown in Figure 3. Even in Figure 4, the three vehicles are connected to each other with a linear topology, however, multihop V2V communication can accommodate any network topology (i.e., an arbitrary graph) over VANET routing protocols.

>>> so in this section, I'd expect to see a Vehicle communicating with another one and using either line of sight or V2V relaying but also using relay via V2I (multihop I2I not just hub and spoke V2I2V), alternatively to together for redundancy. Is that part of the problem?
==> [PAUL] Yes, this is one of the problems stated in this draft. In addition, we removed OMNI interface stuff here for simplicity.

Section 4.3

OLD
Figure 4 shows the internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal

network (Moving Network2) inside Vehicle2. Vehicle2 has two hosts (Host3 and Host4), and two routers (IP-OBU2 and Router2). Vehicle1's IP-OBU1 (as a mobile router) and Vehicle2's IP-OBU2 (as a mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. ~~Alternatively, Vehicle1 and Vehicle2 employ an OMNI interface and use IPv6 ULAs for V2V networking.~~ Thus, a host (Host1) in Vehicle1 can communicate with another host (Host3) in Vehicle2 for a vehicular service through Vehicle1's moving network, a wireless link between IP-OBU1 and IP-OBU2, and Vehicle2's moving network.

==> [PAUL] We add Figure 5 and the text for V2I2V as follows.

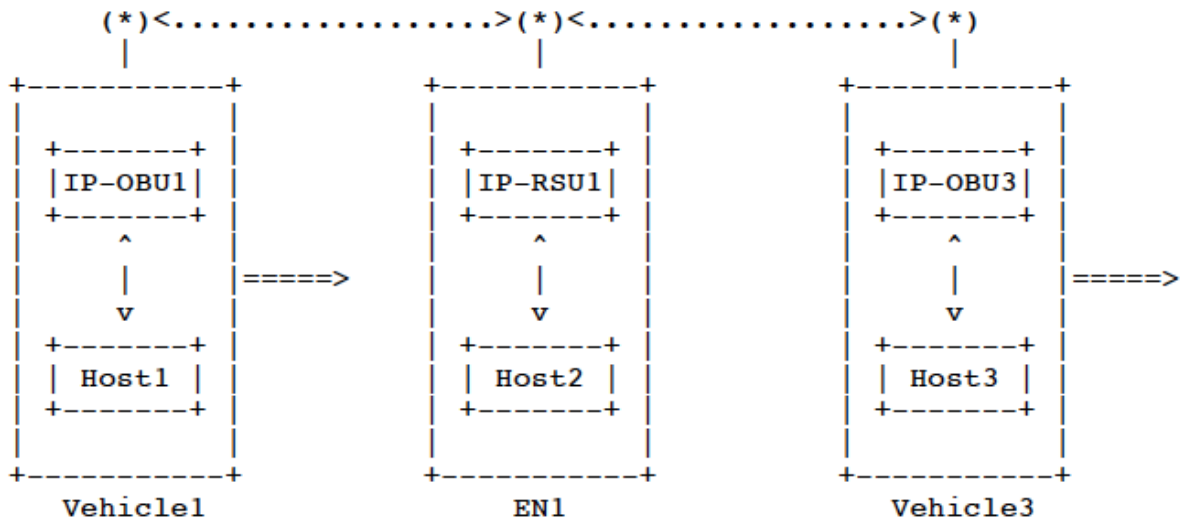


Figure 5: Multihop Internetworking between Two Vehicle Networks via IP-RSU (V2I2V)

Section 4.3

OLD
As shown in Figure 5, multihop internetworking between two vehicles is feasible via an infrastructure node (i.e., IP-RSU) with wireless connectivity among the moving networks of two vehicles and the fixed network of an edge network (denoted as EN1) in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-RSU1 in EN1, and IP-OBU3 in Vehicle3 in the VANET, as shown in the figure.

>>> reading deeper section 5 I found excellent text on routing via V and via I. This tells that section 4 does not play a good role at justifying section 5. Maybe keep section 4 for another doc?
==> [PAUL] Thanks for the comment. We keep Section 4 for the cornerstone for Section 5. Without Section 4, it is hard for the audience to imagine what vehicular networks look like.

>>> What kind or reliability is required in a V2V use case? Do you think ND can handle it? Or MANET? What would be the assumption on L2 (roaming time, unicast vs P2MP) and on L3 (reliability ala DetNet/RAW). Should we have some L3 redundancy?
==> [PAUL] The classical IPv6 ND has some limitations to the V2V case, which is discussed in Section 5.1.

The ND optimization defined in MANET [RFC6130][RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the difference versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181] [RFC7188] [RFC7722] [RFC7779] [RFC8218] and the Dynamic Link Exchange Protocol (DLEP) with its extensions [RFC8175] [RFC8629] [RFC8651] [RFC8703] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services.

For the reliability in V2V networking, some redundancy mechanisms should be provided in L3 in the case of the failure of L2. We updated the text for a more clear description as follows.

Section 4.3

NEW
For the reliability required in V2V networking, the ND optimization defined in MANET [RFC6130][RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the difference versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181] [RFC7188] [RFC7722] [RFC7779] [RFC8218] and the Dynamic Link Exchange Protocol (DLEP) with its extensions [RFC8175] [RFC8629] [RFC8651] [RFC8703] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in the case of the failure of L2.

<snip>

5. Problem Statement

<snip>

In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively short compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles.

>>> Any order of magnitude?
==> [PAUL] For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges.

Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is 72 seconds, and the lifetime of a link between two vehicles is 36 seconds. In reality, the DSRC communication range is around 500m, so the link lifetime will be a half of the maximum time. Thus, IPv6 protocol exchanges need to be done as short as possible to support the message exchanges of various applications in vehicular networks. This explanation is reflected in Section 5 as follows.

Section 5

NEW
For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is 72 seconds, and the lifetime of a link between two vehicles is 36 seconds. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. This relative speed leads the half of the link lifetime between the vehicle and the IP-RSU. In reality, the DSRC communication range is around 500m, so the link lifetime will be a half of the maximum time. The time constraint of a wireless link between two nodes (e.g., vehicle and IP-RSU) needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's type such as a web surfing, voice call over IP, DNS query, and context-aware navigation (in Section 3.1). Regardless of a session's type, to guide all the IPv6 packets to their destination host(s), IP mobility should be supported for the session. In a V2V scenario (e.g., context-aware navigation), the IPv6 packets of a vehicle should be delivered to relevant vehicles in an efficient way (e.g., multicasting). With this observation, IPv6 protocol exchanges need to be done as short as possible to support the message exchanges of various applications in vehicular networks.

>>> Can you indicate whether this already rules out certain procedures, e.g. DAD ?
==> [PAUL] We do not necessarily rule out certain procedures like DAD, but such procedures can be omitted by the help of infrastructure (e.g., DHCPv6) and a unique prefix allocation per vehicle. This is discussed in Mobility Management in Section 5.2.

Section 5.2

OLD
For a mobility management scheme in a shared domain, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link, the DAD is not required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213]), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique. There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management.

The lifetime of a session varies depending on the session's type such as a web surfing, voice call over IP, and DNS query. Regardless of a session's type, to guide all the IPv6 packets to their destination host, IP mobility should be supported for the session.

>>> this seems to be for unicast when you know who to talk to. Is there a need some multicast groups like anybody around interested in topic blah like I could be multicasting the speed of vehicles coming the other way that I crossed recently, for use of vehicles that I'm crossing now, so they can see a slowdown on advance
==> [PAUL] This could be a potential requirement or issue for the multicast function in IPv6-based V2V communications. We address this comment in the text as follows.

Section 5

NEW
For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is 72 seconds, and the lifetime of a link between two vehicles is 36 seconds. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. This relative speed leads the half of the link lifetime between the vehicle and the IP-RSU. In reality, the DSRC communication range is around 500m, so the link lifetime will be a half of the maximum time. The time constraint of a wireless link between two nodes (e.g., vehicle and IP-RSU) needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's

type such as a web surfing, voice call over IP, DNS query, and context-aware navigation (in Section 3.1). Regardless of a session's type, to guide all the IPv6 packets to their destination host(s), IP mobility should be supported for the session. In a V2V scenario (e.g., context-aware navigation), the IPv6 packets of a vehicle should be delivered to relevant vehicles in an efficient way (e.g., multicasting). With this observation, IPv6 protocol exchanges need to be done as short as possible to support the message exchanges of various applications in vehicular networks.

Thus, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. This section presents key topics such as neighbor discovery and mobility management.

>>> Only ND? What about the MANET?

==> [PAUL] We consider the ND in MANET. We have described some limitations in MANET ND in Section 4.3, which may resolve this comment.

Section 4.3

NEW
For the reliability required in V2V networking, the ND optimization defined in MANET [RFC6130][RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the difference versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181] [RFC7188] [RFC7722] [RFC7779] [RFC8218] and the Dynamic Link Exchange Protocol (DLEP) with its extensions [RFC8175] [RFC8629] [RFC8651] [RFC8703] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in the case of the failure of L2.

>>> how fast should ND be to be suitable?

==> [PAUL] We are not sure how fast the ND shall be in the vehicular networks, but the ND protocol exchanges should be done as quickly as possible. We have already addressed the IPv6 protocol exchanges including ND as follows.

Section 5

NEW
For safe driving, vehicles need to exchange application messages every 0.5 second

[NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is 72 seconds, and the lifetime of a link between two vehicles is 36 seconds. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. This relative speed leads the half of the link lifetime between the vehicle and the IP-RSU. In reality, the DSRC communication range is around 500m, so the link lifetime will be a half of the maximum time. The time constraint of a wireless link between two nodes (e.g., vehicle and IP-RSU) needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's type such as a web surfing, voice call over IP, DNS query, and context-aware navigation (in Section 3.1). Regardless of a session's type, to guide all the IPv6 packets to their destination host(s), IP mobility should be supported for the session. In a V2V scenario (e.g., context-aware navigation), the IPv6 packets of a vehicle should be delivered to relevant vehicles in an efficient way (e.g., multicasting). With this observation, IPv6 protocol exchanges need to be done as short as possible to support the message exchanges of various applications in vehicular networks.

>>> is there also a bandwidth check? You can make things much faster if you dedicate a lot of spectrum to it. But that can also be a waste.

==> [PAUL] The bandwidth is determined by link layer and PHY layer, and the upper layers can obtain the bandwidth information from the lower layers. For a DSRC-based interface, the current IEEE 802.11-OCB regulates several bandwidths such as 3Mbps, 6Mbps, and 18Mbps with respect to different MCSes (Modulation and Coding Scheme). This could be an optimization point by selecting a bandwidth for different types of traffic. Note that usually the higher bandwidth gives the shorter communication range and the higher packet error rate at the receiving side, which may reduce the reliability of the IPv6 protocol message transmission. We updated the text to mention the bandwidth case as follows.

Section

OLD
Thus, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. This section presents key topics such as neighbor discovery and mobility management.

Section

NEW
Thus, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery

(ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. Meanwhile, the bandwidth of the wireless link determined by the lower layers (i.e., link and PHY layers) can affect the transmission time of control messages of the upper layers (e.g., IPv6) and the continuity of sessions in the higher layers (e.g., IPv6, TCP, and UDP). Hence the bandwidth selection according to Modulation and Coding Scheme (MCS) also affects the vehicular network connectivity. Note that usually the higher bandwidth gives the shorter communication range and the higher packet error rate at the receiving side, which may reduce the reliability of control message exchanges of the higher layers (e.g., IPv6). This section presents key topics such as neighbor discovery and mobility management for links and sessions in IPv6-based vehicular networks.

5.1. Neighbor Discovery

<snip>

The requirements for IPv6 ND for vehicular networks are efficient DAD and NUD operations.

>>> Not lookup? Is it the intention to use IP unicast over MAC broadcast, which is a good idea in my book?

<snip>

This merging and partitioning should be considered for the IPv6 ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862].

>>> Not lookup? Is it the intention to use IP unicast over MAC broadcast, which is a good idea in my book?
==> For the two above comments, a lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) since some IPv6 addresses have been registered in an MA or IP-RSU for both DAD and NUD operations.

Section 5.1

NEW
The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks. The merging and partitioning of VANETs frequently occurs in vehicular networks. This merging and partitioning should be considered for the IPv6

ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the uniqueness of an IPv6 address that will be configured by a vehicle as DAD. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the existence of a vehicle under the network coverage of the MA or IP-RSU as NUD. Thus, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs, and IPv6 ND needs to detect unreachable neighboring vehicles due to the partitioning of a VANET. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or an off-link host even though the source vehicle can use the same prefix as the destination vehicle [ID-IPPL].

<snip>

Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. Also, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or an off-link host even though the source vehicle uses the same prefix as the destination vehicle.

>>> should reference to draft-nordmark-intarea-ippl

==> [PAUL] We cited draft-nordmark-intarea-ippl as [ID-IPPL] for the text and put it in the informative references.

Section 5.1

NEW
The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks. The merging and partitioning of VANETs frequently occurs in vehicular networks. This merging and partitioning should be considered for the IPv6 ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the uniqueness of an IPv6 address that will be configured by a vehicle as DAD. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the existence of a vehicle under the network coverage of the MA or IP-RSU as NUD. Thus, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs, and IPv6 ND needs to detect unreachable

neighboring vehicles due to the partitioning of a VANET. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or an off-link host even though the source vehicle can use the same prefix as the destination vehicle [ID-IPPL].

To efficiently prevent IPv6 address duplication due to the VANET partitioning and merging from happening in vehicular networks, the vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD. In this case, two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and IP-RSUs, as shown in Figure 1. By using the vehicular-network-wide DAD, vehicles can assure that their IPv6 addresses are unique in the vehicular network whenever they are connected to the vehicular infrastructure or become disconnected from it in the form of VANET.

>>> Excellent
==> [PAUL] Thanks!

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles.

>>> Is that a problem or just an operational setting that needs to be found?
>>> Do we need to reconsider the concepts of those timers?
==> [PAUL] At the moment, the ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks.

Section 5.1

OLD
ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles.

Section 5.1

NEW

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles. The ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks.

<snip>

Thus, in IPv6-based vehicular networking, IPv6 ND should have minimum changes for the interoperability with the legacy IPv6 ND used in the Internet, including the DAD and NUD operations.

>>> I do not find the logical link with the text before, why is this a "thus"?
==> [PAUL] We delete "thus".

>>> why should the ND inside the VANET be constrained to be interoperable? This may place constraints on the solution.
==> [PAUL] We modified this paragraph to make it more logical to connect the previous paragraph.

For the 2nd comment, here we do not separate a VANET domain from the Internet domain, which means any vehicle inside a VANET domain shall have the standard IPv6 ND process that can guarantee the Internet connection once it is on-link. The minimum changes to the IPv6 ND mean that they support the seamless connectivity of vehicles to other intelligent transportation elements. We address this as follows.

Section 5.1

OLD
Thus, in IPv6-based vehicular networking, IPv6 ND should have minimum changes ~~for the interoperability~~ with the legacy IPv6 ND used in the Internet, including the DAD and NUD operations.

Section 5.1

NEW
From the interoperability point of view, in IPv6-based vehicular networking, IPv6 ND should have minimal changes with the legacy IPv6 ND used in the Internet, including the DAD and

NUD operations, so that IPv6-based vehicular networks can be seamlessly connected to other intelligent transportation elements (e.g., traffic signals, pedestrian wearable devices, electric scooters, and bus stops) that use the standard IPv6 network settings.

5.1.1. Link Model

A prefix model for a vehicular network needs to facilitate the

>>> Do you mean a "subnet model" as opposed to "prefix model".
>>> it would make this piece and the next should refer to draft-thubert-6man-ipv6-over-wireless for IPv6 over P2MP /NBMA, for both link and subnet issues. The general ideas are the same, but the gory details here are slightly incorrect, like this notion of prefix model than comes out of the blue. The model is really the subnet model for the subnet associated to P2MP.
==> [PAUL] Here a prefix model for the IPv6-based vehicular networks particularly means the IPv6 address configuration model based on IPv6 prefix(s). To remove the confusion, we replaced it with "a subnet model". We also added draft-thubert-6man-ipv6-over-wireless as a reference for this draft.

Section 5.1.1

OLD
A prefix model for a vehicular network needs to facilitate the communication between two vehicles with the same prefix regardless of the vehicular network topology as long as there exist bidirectional E2E paths between them in the vehicular network including VANETs and IP-RSUs. This prefix model allows vehicles with the same prefix to communicate with each other via a combination of multihop V2V and multihop V2I with VANETs and IP-RSUs. Note that the OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD messaging.

Section 5.1.1

NEW
A subnet model for a vehicular network needs to facilitate the communication between two vehicles with the same prefix regardless of the vehicular network topology as long as there exist bidirectional E2E paths between them in the vehicular network including VANETs and IP-RSUs. This subnet model allows vehicles with the same prefix to communicate with each other via a combination of multihop V2V and

multihop V2I with VANETs and IP-RSUs. [IPoWIRELESS] introduces other issues in an IPv6 subnet model.

communication between two vehicles with the same prefix regardless of the vehicular network topology as long as there exist bidirectional E2E paths between them in the vehicular network including VANETs and IP-RSUs. This prefix model allows vehicles with the same prefix to communicate with each other via a combination of multihop V2V and multihop V2I with VANETs and IP-RSUs. Note that the OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD messaging.

>>> again overselling OMNI.
>>> I kinda agree about the OMNI interface model, nothing against that. But you must see that there needs a lot more than what the OMNI interface to get packets across V and I hops to the destination. Like routing ala MANET, redundancy handling ala DetNet because it will be very lossy, path management ala RAW to optimize delivery vs. spectrum… And OMNI ignores ND so it does not solve the ND problems above.
==> [PAUL] We removed the contents related to OMNI here.

Section 5.1.1

NEW
~~Note that the OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD messaging.~~

IPv6 protocols work under certain assumptions that do not necessarily hold for vehicular wireless access link types other than OMNI/NBMA [VIP-WAVE][RFC5889]; the rest of this section discusses implications for those link types that do not apply when the OMNI/NBMA link model

>>> again overselling OMNI.
>>> The keyword here is P2MP / NBMA, and OMNI is one interface that accepts that. There are others. IBM's IPv4 over Frame relay was already P2MP / NBMA, using routing to complete the partial mesh in P2MP. The text seems to imply that OMNI is the only way to do that and that's wrong. Also OMNI is loaded with other stuff than a plain P2MP capable interface. And ND over P2MP is not done by OMNI, OMNI only makes classical ND worse and only works in a full mesh. OTOH RFC 8505, which is designed to do ND for P2MP /NBMA would indeed work very well within an OMNI interface and solve those problems.

>>> My point is that you need to tell the full story or refrain from entering solution space in this doc
==> [PAUL] To reduce the confusion, we removed the OMNI stuff here.

Section 5.1.1

NEW
IPv6 protocols work under certain assumptions that do not necessarily hold for vehicular wireless access link types ~~other than OMNI/NBMA~~ [VIP-WAVE][RFC5889]~~; the rest of this section discusses implications for those link types that do not apply when the OMNI/NBMA link model is used~~. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [RFC6250]. However, radio interference and different levels of transmission power may cause asymmetric links to appear in vehicular wireless links. As a result, a new vehicular link model needs to consider the asymmetry of dynamically changing vehicular wireless links.

<snip>

There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IPv6 link.

>>> not assumed; that's what the onlink but set tells. The conclusion should be that the VANET cannot set the O bit
==> [PAUL] We agree with the reviewer's comment here. We modified the text to reflect this point.

Section 5.1.1

OLD
There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IPv6 link.

Section 5.1.1

NEW

There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is defined that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IPv6 link.

However, the vehicular link model needs to define the relationship between a link and a prefix, considering the dynamics of wireless links and the characteristics of VANET.

<snip>

From the previous observation, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use an on-link prefix and off-link prefix according to the network topology of vehicles such as a one-hop reachable network and a multihop reachable

>>> No, the once a node saw a O bit set that sticks even if it sees other advertisements of the PIO with the O bit not set.
>>> This is a global and intrinsic property of the prefix (and an attack vector that could be mentioned in the sec section).
>>> the VANET prefix must never come with the O bit set.

==> [PAUL] We explain that off-link prefixes will be used for vehicles as default. We have described the security issues for the prefix-based IPv6 address configuration in Section 6. We address this answer as follows.

Section 5.1.1

NEW
From the previous observation, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use an on-link prefix and off-link prefix according to the network topology of vehicles such as a one-hop reachable network and a multihop reachable network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should be off-link. In most cases in vehicular networks, due to the partitioning and merging of VANETs, and the multihop network topology of VANETS, off-link prefixes will be used for vehicles as default.

<snip>

network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link.

>>>> No, see above; but the router may redirect though it is really risky unless this is a stable situation like a parking place.
==> [PAUL] We answered this comment in the previous comment.

Thus, in IPv6-based vehicular networking, the vehicular link model should have minimum changes for interoperability with standard IPv6 links in an efficient fashion to support IPv6 DAD, MLD and NUD operations. When the OMNI NBMA link model is used, there are no link model changes nor DAD/MLD messaging required.

>>>> again overselling OMNI.
>>>> You need a good P2MP subnet model with routing support when the mesh is partial. My company alone has been shipping million of nodes that build subnets of thousands, and that was done using IETF standards.
==> [PAUL] We removed the contents related to OMNI here.

Section 5.1.1

OLD
Thus, in IPv6-based vehicular networking, the vehicular link model should have minimum changes for interoperability with standard IPv6 links in an efficient fashion to support IPv6 DAD, MLD and NUD operations. ~~When the OMNI NBMA link model is used, there are no link model changes nor DAD/MLD messaging required.~~

Section 5.1.1

NEW
Thus, in IPv6-based vehicular networking, the vehicular link model should have minimum changes for interoperability with standard IPv6 links in an efficient fashion to support IPv6 DAD, MLD and NUD operations.

<snip>

For vehicular networks with high mobility and density, the DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange a driving safety message (e.g., collision avoidance and accident notification) with each other with a short

interval (e.g., 0.5 second) by a technical report from NHTSA (National Highway Traffic Safety Administration) [NHTSA-ACAS-Report]. Such a driving safety message may include a vehicle's mobility information (i.e., position, speed, direction, and acceleration/ deceleration). The exchange interval of this message is 0.5 second, which is required to allow a driver to avoid a rear-end crash from another vehicle.

>>> IPv6 over broadcast MAC (used to be called internet 0, 10+ years ago) solves that MAC issue since there is no MAC.
==> [PAUL] Thanks for pointing this out. After checking the context here, the paragraph is moved to Section 5.1 (Neighbor Discovery), since it mainly describes the efficiency issue of DAD. Meanwhile, we update some text for simplicity.

Section 5.1

OLD
For vehicular networks with high mobility and density, the DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange ~~a~~ driving safety message (e.g., collision avoidance and accident notification) with each other with a short interval (e.g., 0.5 second) by a technical report from NHTSA (National Highway Traffic Safety Administration) [NHTSA-ACAS-Report]. ~~Such a~~ driving safety message may include a vehicle's mobility information (i.e., position, speed, direction, and acceleration/deceleration). The exchange interval of this message is 0.5 second, which is required to allow a driver to avoid a rear-end crash from another vehicle.

Section 5.1

NEW
For vehicular networks with high mobility and density, the DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange driving safety messages (e.g., collision avoidance and accident notification) with each other with a short interval suggested by NHTSA (National Highway Traffic Safety Administration) [NHTSA-ACAS-Report]. Since the partitioning and merging of vehicular networks may require re-perform the DAD process repeatedly, the link scope of vehicles may be limited to a small area, which may delay the exchange of driving safety messages. Driving safety messages can include a vehicle's mobility information (i.e., position, speed, direction, and acceleration/deceleration) that is critical to other vehicles. The exchange interval of this message is recommended to be less than 0.5 second, which is required for a driver to avoid an emergency situation, such as a rear-end crash.

5.1.3. Routing

For multihop V2V communications in either a VANET or VANETs via IP-RSUs, a vehicular Mobile Ad Hoc Networks (MANET) routing protocol may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will

be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [ID-Multicast-Problems].

>>> we do that with IETF standards on battery operated devices already. Using RFC 8505 for the UNI and RPL for the NNI. It is scalable (we've seen 30 hops in meshes of thousands in the real world though it's not the normal operational model, but can happen to maintain connectivity during the reboot of a root) and does not use broadcast. RPL was initially designed as a V2V2V protocol but found its market on the IoT. I'm sure the protocol would gladly come back to its roots.
==> [PAUL] Thanks for pointing this out. We discuss the limitations for RFC8505 and RPL in the text as follows.

Section 5.1

NEW
RPL can use the information provided by the extended ARO defined in [RFC8505] to deal with a certain level of node mobility. When a leaf node moves to the coverage of another parent node, it should de-register its addresses to the previous parent node and register itself with a new parent node along with an incremented TID. Although RPL can be used in IPv6-based vehicular networks, it is primarily designed for lossy networks, which puts energy efficiency first. In addition, the topology it considers may not quickly scale up and down for IPv6-based vehicular networks, since the mobility of vehicles is much more diverse with a high speed, so it can frequently alter a tree-like topology formed by RPL, which may cause network fragmentation and merging with more control traffic. Moreover, due to bandwidth and energy constraints, RPL does not suggest to use a proactive mechanism (e.g., keepalive) to maintain accurate routing adjacencies such as Bidirectional Forwarding Detection [RFC5881] and MANET Neighborhood Discovery Protocol [RFC6130]. As a result, due to the mobility of vehicles, the network fragmentation is not detected quickly and the routing of packets between vehicles or between a vehicle and an infrastructure node may fail.

A routing protocol for a VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in a VANET with a dynamic network topology because the IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of the IPv6 ND to minimize its control overhead.

>>> A clean description of the interaction of RPL and RFC 8505 in our IoT networks. Note that the speed of the PHY in VANET balanced the instability of the topology, and RPL still applies. Note also that RPL uses DV with a routing stretch in order to minimize the topology awareness that's needed in each node, which results in minimal signaling.

==> [PAUL] We updated this section to have the description of RPL and its applicability to vehicular networks as follows:

Section 5.1.3

OLD
A routing protocol for a VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in a VANET with a dynamic network topology because the IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of the IPv6 ND to minimize its control overhead.

Section 5.1.3

NEW
For multihop V2V communications in either a VANET or VANETs via IP-RSUs, a vehicular Mobile Ad Hoc Networks (MANET) routing protocol may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [ID-Multicast-Problems]. A routing protocol for a VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in a VANET with a dynamic network topology because the IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of the IPv6 ND to minimize its control overhead. RPL [RFC6550] defines a routing protocol for low-power and lossy networks, which constructs and maintains DODAGs optimized by an Objective Function (OF). A defined OF provides route selection and optimization within a RPL topology. A node in a DODAG uses DODAG Information Objects (DIOs) messages to discover and maintain the upward routes toward the root node. An address registration extension for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) in [RFC8505] can support light-weight mobility for nodes moving through different parents. Mainly it updates the Address Registration Option (ARO) of ND defined in [RFC6775] to include a status field that can indicate the movement of a node and optionally a Transaction ID (TID) field, i.e., a sequence number that can be used to determine the most recent location of a node.

RPL can use the information provided by the extended ARO defined in [RFC8505] to deal with a certain level of node mobility. When a leaf node moves to the coverage of another parent node, it should de-register its addresses to the previous parent node and register itself with a new parent node along with an incremented TID.

Although RPL can be used in IPv6-based vehicular networks, it is primarily designed for lossy networks, which puts energy efficiency first. In addition, the topology it considers may not quickly scale up and down for IPv6-based vehicular networks, since the mobility of vehicles is much more diverse with a high speed, so it can frequently alter a tree-like topology formed by RPL, which may cause network fragmentation and merging with more control traffic.

Moreover, due to bandwidth and energy constraints, RPL does not suggest to use a proactive mechanism (e.g., keepalive) to maintain accurate routing adjacencies such as Bidirectional Forwarding Detection [RFC5881] and MANET Neighborhood Discovery Protocol [RFC6130]. As a result, due to the mobility of vehicles, the network fragmentation is not detected quickly and the routing of packets between vehicles or between a vehicle and an infrastructure node may fail.

5.2. Mobility Management

<snip>

For a mobility management scheme in a shared link, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link,

>>> I would not use the term link, or shared. Maybe shared link -> domain?
==> [PAUL] We updated the term “shared link” here with “domain” to remove confusion.

Section 5.2

OLD
For a mobility management scheme in a shared link, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link, the DAD is not required.

Section 5.2

NEW
For a mobility management scheme in a domain, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link, the DAD is not required.

<snip>

the DAD is not required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213] and OMNI [OMNI]), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique.

>>> again overselling OMNI
>>> As I said earlier, this is wring there are (64*) more chances of a collision in OMNI prefixes than in IPv6 IIDs.
>>> OMNI prefixes can collision, home addresses that are unique on a home network cannot.
>>> Now if both the OMNI prefix and the IID are good randoms, then obviously, the chances of collisions round up to 0.
>>> Collision is certainly not my worst fear.
==> [PAUL] We removed the reference here to OMNI.

Section 5.2

NEW
For a mobility management scheme in a shared link, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link, the DAD is not required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213] ~~and OMNI [OMNI]~~), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique. There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management.

There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management.

>>> This is way too superficial and hides the reality of things.
- Using a VANET Infra prefix allows direct routability to the internet which BYOA does not since the BYOA is not topologically correct. Yes, it costs a DAD with classic ND, but it does not with RCF8505 and the draft fails to mention that.
- A BYOA needs a tunnel home, and the node needs to know who is reachable inside the VANET and what is not to decide to tunnel or not; this is a difficult problem (vs. control place overhead) that is not discussed here.
==> [PAUL] We describe the operations defined in RFC8505 in Section 5.1.3 as follows.

Section 5.2

OLD
There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management.

Section 5.2

NEW
There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management. Even though the SLAAC with classic ND costs a DAD during mobility management, the SLAAC with [RFC8505] does not cost a DAD. SLAAC for vehicular networks needs to consider the minimization of the cost of DAD with the help of an infrastructure node (e.g., IP-RSU and MA). Using an infrastructure prefix over VANET allows direct routability to the Internet through the multihop V2I toward an IP-RSU. On the other hand, a BYOA does not allow such direct routability to the Internet since the BYOA is not topologically correct, that is, not routable in the Internet. In addition, a vehicle configured with a BYOA needs a tunnel home (e.g., IP-RSU) connected to the Internet, and the vehicle needs to know which neighboring vehicle is reachable inside the VANET toward the tunnel home. There is nonnegligible control overhead to set up and maintain routes to such a tunnel home over the VANET.

<snip>

For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC8028]. That is, the vehicle should select its default router for each prefix by preferring the router that advertised the prefix.

>>> Still router discovery (in and out) must be very fast. Thing of the RA intervale in MIPv6. Is that sufficient? Too expensive?
==> [PAUL] We describe the multihomed network case for vehicular networks to reflect a comment given by the previous reviewer (Erik Nordmark). To clarify this point, we updated the text as follows.

For multihomed networks, RFC 8028 specifies the guidelines for a host that has multiple prefixes given by an upstream network, e.g., connected to a multi-interface router. For vehicular networks, an IP-OBU inside a vehicle may connect to an IP-RSU that has multiple routers behind. In this scenario, because the IP-OBU can have multiple prefixes from those routers, the default router selection, source address selection, and packet redirect process should follow the guidelines in RFC 8028.

We updated the text here for a more clear description as follows.

Section 5.2

OLD
For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC8028]. That is, the vehicle should select its default router for each prefix by preferring the router that advertised the prefix.

Section 5.2

NEW
For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC8028]. For example, an IP-OBU inside a vehicle may connect to an IP-RSU that has multiple routers behind or multiple IP-RSUs. In this scenario, because the IP-OBU can have multiple prefixes from those routers, the default router selection, source address selection, and packet redirect process should follow the guidelines in [RFC 8028]. That is, the vehicle should select its default router for each prefix by preferring the router that advertised the prefix.

<snip>

6. Security Considerations

>>> Any discussion on the security of classical ND and other operational issues (rfc6583) ?
==> [PAUL] We added a new paragraph to describe the security issues in the classical ND.

Meanwhile, we also re-organized the structure of Section 6 to categorize different security threats from ND, mobility management, and other aspects.

Section 6.1

NEW
6.1. Security Threats in Neighbor Discovery For the classical IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6loWPAN ND from address theft and impersonation attacks. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based approach [Vehicular-BlockChain] can be used. However, for a scenario where a trustable router or an authentication path can not be obtained, it is desirable to find a solution in which vehicles and infrastructures can authenticate each other without any support from a third party. When applying the classical IPv6 ND process to VANET, one of the security issues is that an IP-RSU (or an IP-OBU) as a router may receive deliberate or accidental DoS attacks from network scans that probe devices on a VANET. In this scenario, the IP-RSU can be overwhelmed for processing the network scan requests so that the capacity and resources of IP-RSU are exhausted, causing the failure of receiving normal ND messages from other hosts for network address resolution. [RFC6583] describes more about the operational problems in the classical IPv6 ND mechanism that can be vulnerable to deliberate or accidental DoS attacks and suggests several implementation guidelines and operational mitigation techniques for those problems. Nevertheless, for running IPv6 ND in VANET, those issues can be more acute since the movements of vehicles can be so diverse that it leaves a large room for rogue behaviors, and the failure of networking among vehicles may cause grave consequences.

<snip>

Security and privacy are paramount in V2I, V2V, and V2X networking. Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. Also, in-vehicle devices (e.g., ECU) and a driver/passenger's mobile devices (e.g., smartphone and tablet PC) in a vehicle need to communicate with other in-vehicle devices and another driver/passenger's mobile devices in another vehicle, or other servers behind an IP-RSU in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be required to reduce the aftermath of malicious behaviors.

>>> The section should mention that both with classical ND and BYOA, addresses can be impersonated, and RFC 8928 protects against that in both cases while maintaining privacy.
==> [PAUL] The previous modifications have reflected this comment. We also referred to RFC 8928 in Section 6.1 to give the information.

Section 6.1

NEW
6.1. Security Threats in Neighbor Discovery For the classical IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6loWPAN ND from address theft and impersonation attacks. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based approach [Vehicular-BlockChain] can be used. However, for a scenario where a trustable router or an authentication path can not be obtained, it is desirable to find a solution in which vehicles and infrastructures can authenticate each other without any support from a third party.

Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated

>>> Is PKI feasible (deploying it in every car?). Is it fast enough? Is it really what IPWAVE thinks vehicle should use?????
>>> e.g. why would one need to authenticate to a V2I network?
>>> from the text earlier in the doc, it seemed that what you really want is access that is fast to join, capable of offering the reachability you want, anonymous, and innocuous (cars can not harm one another).
==> [PAUL] For PKI, we can say that this is a way, though it requires additional steps to reach the goal. For some intelligent transportation services, e.g., vehicle navigation and traffic flow control, a malicious (or compromised) vehicle may send counterfeit information toward a remote server. That is why we need to authenticate a vehicle.

Although cars cannot harm one another directly, some information that a car shares is important to others and if the information is fabricated, other cars may be misguided, in particular for some safety applications discussed in Section 3. We address this comment as follows.

Section 6

OLD
Security and privacy are paramount in V2I, V2V, and V2X networking. Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. Also, in-vehicle devices (e.g., ECU) and a driver/passenger's mobile devices (e.g., smartphone and tablet PC) in a vehicle need to communicate with other in-vehicle devices and another driver/passenger's mobile devices in another vehicle, or other servers behind an IP-RSU in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be required to reduce the aftermath of malicious behaviors.

Section 6

NEW
Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a kind of Public Key Infrastructure (PKI) in an efficient way. To provide safe interaction between vehicles or between a vehicle and infrastructure, only authenticated nodes (i.e., vehicle and infrastructure node) can participate in vehicular networks. Also, in-vehicle devices (e.g., ECU) and a driver/passenger's mobile devices (e.g., smartphone and tablet PC) in a vehicle need to communicate with other in-vehicle devices and another driver/passenger's mobile devices in another vehicle, or other servers behind an IP-RSU in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be required to reduce the aftermath of malicious behaviors.

vehicles may harm other vehicles, so their communication activities need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

>>> solution space; better express the security needs since this is a PS.
==> [PAUL] We modified the text here to emphasize problems.

Section 6

OLD
Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles, so their communication activities need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

Section 6

NEW
Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of

each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of “zero-trust” for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero trust framework or mechanism for vehicular networks.

For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

<snip>

To identify malicious vehicles among vehicles, an authentication method is required.

>>> No. As said earlier a vehicle can be infected. You need innocuousness.which can come from things like isolation, zero trust, and protocols that are difficult to hack around. Classical IPv6 ND is open bar. RFC 8505/8928 is protected by construction, anonymous, and fast.
==> [PAUL] We modified the description here, and along with the previous modifications, we have added the issues to have innocuous vehicular networks in Section 6.3.

Section 6.1

OLD
To identify malicious vehicles among vehicles, an authentication method is required.

Section 6.1

NEW
To identify malicious vehicles among vehicles, an authentication method may be required.

==> [PAUL] We discuss the concept of “zero-trust” as follows.

Section 6.3

NEW
6.3. Other Threats For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC or 5G V2X (or LTE V2X) is required in a highway. In this case, multiple intermediate vehicles as relay nodes can help forward association and authentication messages toward an IP-RSU (gNodeB, or eNodeB) connected to an authentication server in the vehicular cloud. In this kind of process, the authentication messages forwarded by each vehicle can be delayed or lost, which may increase the construction time of a connection or some vehicles may not be able to be authenticated. Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.

<snip>

For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC is required in a highway for the authentication by involving multiple intermediate vehicles as relay nodes toward an IP-RSU connected to an authentication server in the vehicular cloud. The V2I communications over 5G V2X (or LTE V2X) is required to allow a vehicle to communicate directly with a gNodeB (or eNodeB) connected to an authentication server in the vehicular cloud.

>>> solution space. Instead, you could mention that setting up secured channels between cars that cross one another might not complete in time to establish the communication channel, and that the innocuousness must come from zero trust in the transactions between the cars. For the IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface.
>>> for classical ND (SLAAC) that's true. That is not with RFC 8505, since the infra maintains a table of all addresses in use in the prefix and blocks duplicates without the RFC 4862 DAD method. The stateful autoconf address grant is immediate.
==> [PAUL] We agree to this point. We modified the description to remove the confusion as follows.

Section 6

OLD
For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC is required in a highway for the authentication by involving multiple intermediate vehicles as relay nodes toward an IP-RSU connected to an authentication server in the vehicular cloud. ~~The V2I communications over 5G V2X (or LTE V2X) is required to allow a vehicle to communicate directly with a gNodeB (or eNodeB) connected to an authentication server in the vehicular cloud.~~

Section 6

NEW
For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC or 5G V2X (or LTE V2X) is required in a highway. In this case, multiple intermediate vehicles as relay nodes can help forward association and authentication messages toward an IP-RSU (gNodeB, or eNodeB) connected to an authentication server in the vehicular cloud. In this kind of process, the authentication messages forwarded by each vehicle can be delayed or lost, which may increase the construction time of a connection or some vehicles may not be able to be associated authenticated.

This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks.

>>> also for DOS attacks. You can block a owner from using an address. A reference to rfc6959 is much needed here.
==> [PAUL] We cite RFC6959 and RFC8928 for ND-related attacks and countermeasures. We discuss the main contents and roles of RFC6959 and RFC8928 as follows.

Section 6

OLD
For the IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks.

Section 6.1

NEW

For the classical IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6loWPAN ND from address theft and impersonation attacks.

<snip>

This possibility indicates that the vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based mechanism [Vehicular-BlockChain] can be used.

>>> solution space. Again, the draft should focus on problems and needs. The problem here is that SEND is complex, and not implemented in the major stack. It relies on PKI for trusting the router. The V2I need is a zero trust model here one V, the other local Vs, and the I, can help each other anonymously and harmlessly.
==> [PAUL] Here we first gave the existing classical solutions based on the original text, and then we added a new description for the issue suggested by the reviewer.

Section 6

OLD
For the IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. This possibility indicates that the vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA

Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based mechanism [Vehicular-BlockChain] can be used.

Section 6.1

NEW
For the classical IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6loWPAN ND from address theft and impersonation attacks. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based approach [Vehicular-BlockChain] can be used. However, for a scenario where a trustable router or an authentication path cannot be obtained, it is desirable to find a solution in which vehicles and infrastructures can authenticate each other without any support from a third party.

<snip>

8. Informative References

>>> no normative reference?

>>> no normative reference?
==> [PAUL] We have moved most of RFCs to the Normative References section.

<snip>

Voila!

Keep safe;

Pascal
==========

Thanks for your valuable comments.

Best Regards,
Jaehoon (Paul) Jeong